13 SECURITY TIPS FOR JOURNALISTS COVERING HATE ONLINE

By April Glaser

THE MEDIA MANIPULATION CASEBOOK

13 SECURITY TIPS FOR JOURNALISTS COVERING HATE ONLINE

At the beginning of August 2019, a young white man entered a Walmart in El Paso, Texas, and opened fire with an AK-47-style rifle ordered online, killing 22 people and injuring 25 more. Less than an hour after the shooting was reported, internet researchers found an anti-immigrant essay uploaded to the anonymous online message board 8chan. Law enforcement officials later said that before the shooter opened fire, they were investigating the document, which was posted minutes before the first calls to 911. The essay posted on 8chan included a request: “Do your part and spread this brothers!”

That was the third time in 2019 that a gunman posted a document on 8chan about his intent to commit a mass shooting. All three of the pieces of writing from shooters posted online that year were loaded with white supremacist beliefs and instructions to share their message or any video of the shooting far and wide. The year prior, a man who entered into a synagogue outside of Pittsburgh and opened fire was an active member of online forums popular amongst communities of hate, where he, too, signaled his intent to commit violence before he killed. In 2017, the deadly Unite the Right rally in Charlottesville, Virginia, was largely organized in online forums, too. And so it makes sense that in recent years newsrooms are dedicating more reporters to covering how hate spreads over the internet.

Online hate is not an easy beat. First off, there’s the psychological toll of spending hours in chat rooms and message boards where members talk admiringly about the desire to harm and even kill others based on their race, religion, gender and sexual orientation. Monitoring these spaces can leave a reporter feeling ill, alienated and fearful of becoming desensitized. Secondly, some who congregate in online communities of hate are experts at coordinating attacks and promoting violence against those who they disagree with, including activists and journalists who write about them. Such harassment occurs both online and offline and can happen long after a report is published.

In recent years newsrooms are dedicating more reporters to covering how hate spreads over the internet.

Consider a case from my own experience, where my reporting triggered a harassment campaign. In February 2019, I published an investigation of an e-commerce operation that Gavin McInnes, founder of the far-right men’s group the Proud Boys, whose members have been charged with multiple counts of violence, described as the group’s legal defense fund. During the course of my reporting, multiple payment processors used by the e-commerce site pulled their

services. In the days after the article published, I received some harassment on Twitter, but it quickly petered out. That changed in June, after the host of a popular channel on YouTube and far-right-adjacent blogger Tim Pool made a 25-minute video about my story, accusing me of being a "left-wing media activist." The video has since been viewed hundreds of thousands of times.

Within minutes of Pool's video going live, the harassment began again. A dozen tweets and emails per-minute lit up my phone — some included physical threats and anti-Semitic attacks directed at my family and myself. A slew of fringe-right websites, including Infowars, created segments and blog posts about Pool's video. I received requests to reset my passwords, likely from trolls attempting to hack into my accounts. Users of the anonymous message board 4chan and anonymous Twitter accounts began posting information directing people to find where I live.

What follows is general safety advice for newsrooms and journalists who report on hate groups and the platforms where they congregate online.

Securing yourself before and during reporting

Maintain a strong security posture in the course of your research and reporting in order to prevent potential harassers from finding your personal details. Much of the advice here on how to do that is drawn from security trainers at Equality Labs and Tall Poppy, two organizations that specialize in security in the face of online harassment and threats, as well as my own experience on the beat. It also includes resources that can help newsrooms support and protect reporters who are covering the online hate beat.

Maintain a strong security posture in the course of your research and reporting in order to prevent potential harassers from finding your personal details.

1 Download and begin using a secure password manager.

A password manager is an app that stores all your passwords, which helps with keeping and creating complex and distinct passwords for each account. With your password manager change or reset all your passwords to ensure you're not using the same password across sites and that each password is tough to crack. You probably have more online accounts than you realize, so it might help to make a list. When updating passwords, opt for a two-factor authentication method when available. Use a two-factor authentication app, like Google Authenticator or Duo, rather than text messages, since unencrypted text messages can easily be compromised. 1Password is the password manager of choice for the experts both at Tall Poppy and Equality Labs.

2 Search for your name on online directory and data broker sites.

Sites like White Pages and Spokeo, which collect addresses and contact information that can be sold to online marketers, and request your entries be removed. Online harassment campaigns often start with a search of these sites to find their target's home address, phone number and email. Many data broker sites make partial entries visible, so it's possible to see if your information is listed. If it is, find the site's instructions for requesting removal of your entry and follow the directions. Do the same for people who you live with, especially if they share your last name. There are also services that can thoroughly scrub your identifying information from dozens of online directories across the web for you, like Privacy Duck, Deleteme and OneRep.

3 Make aliases.

If you have to create an account to use a social media site you're researching, consider using an alternate email address that you delete or stop using after the course of reporting. Newsroom practices vary, so if your username must reveal who you are per your employer's policy, check with your editor about using your initials or not spelling out your publication in your username. It's easy to make a free email address using Gmail or Hotmail. ProtonMail also offers free end-to-end encrypted email addresses.

4 Record your interactions with sources, as they may be recording their interactions with you.

Assume every interaction you have is not only being recorded but might also be edited in an attempt to harass you or undercut your work. During one story I worked on about a hate-friendly social network, an employee of the website I interviewed recorded the interview, too. The founder of the site wasn't happy with my report and proceeded to make a Periscope video of him attempting to discredit the story by replaying my interview, courting thousands of views. If you're at a rally, bring spare batteries and ensure you have enough space on your phone to record your interactions or have a colleague with you so you can record each other's interactions, which help if you need evidence to discredit attempts to discredit you. Importantly, before you record any interview, check if the state you're reporting from has a two-party consent law, which requires that both parties on the call consent to being recorded and may require you to alert your interviewee that you're recording the call.

5 Use a Virtual Private Network (VPN) to visit the sites you're investigating.

VPNs hide where web traffic comes from. If you're researching a website and visiting it frequently, your IP address, location or other identifying information could tip off the site's owners that you're poking around. Do your research, as some VPN services are more trustworthy than others. Equality Labs recommends using Private Internet Access. Wirecutter also has a good selection of recommended VPNs.

6 Tighten your social media privacy.

Make sure all your social media accounts are secured with as little identifying information public as possible. Do a scan of who is following you on your personal accounts and that there isn't identifying information about where you live posted in any public place or shared with people who may compromise your safety. Consider unfriending your family members and explain to them why they cannot indicate their relationship to you online. Likewise, be aware of any public mailing lists you may subscribe to where you may have shared your phone number or address in an email and ask the administrator of the email list to remove those emails from the public archive.

7 Ask your newsroom or editor for support.

"Newsrooms have a duty of care to their staff to provide the tools that they need to stay safe," says Leigh Honeywell, the CEO of Tall Poppy. Those tools may include paying for services that remove your information from data broker sites and a high-quality password manager. If your personal information does begin to circulate online, your newsroom should be prepared to contact social media platforms to report abuse and request the information be taken down. Newsroom leadership could also consider implementing internal policies around how to have their reporters' backs in situations of online harassment, which could mean, for example, sifting through threats sent on Twitter and having a front desk procedure that warns anyone who answers the phone not to reveal facts such as whether certain reporters work at the office.

"Newsrooms have a duty of care to their staff to provide the tools that they need to stay safe."

After publishing

If you do face harassment and threats online after your report is published, you may want to enlist the help of an organization that specializes in online harassment security. Troll storms usually run about one week, and the deluge on Twitter and over email usually lasts no more than a few days. Take space from the internet during this time and be sure your editors are prepared to help monitor your accounts should you become a target of harassment.

1 Ask someone to monitor your social media for you.

Depending on the severity and cadence of the harassment that follows publication, you may wish to assign a trusted partner, an editor or a friend, to monitor your social media for you. Often the harassment is targeted at journalists via social media accounts. It can be an extremely alienating experience, especially if consumed through a smartphone, because no one fully sees what's happening except the person targeted. During these moments, it's best to step away from social media and not watch it unfold. This is often hard to do, because it's also important to stay aware of incoming threats or attempts to find your home and family. Whoever is monitoring your social media should report accounts that send harassment, threats, obscenities and bigotry.

2 Don't click on links from unknown senders.

If you receive a text message from an unknown number or an email to reset a password, do not click on any links or open any attachments. Likewise, consider only opening emails in plain-text mode to ensure photos and malicious files do not download automatically. Be extra careful about links in text messages, as it's rare for a password reset to come through a text message and it could be an attempt to verify your phone number by a harasser or to install malware on your phone. If you get suspicious texts or emails, contact whoever you consult for security.

3 Google yourself (or ask someone you trust to Google your name for you).

When the harassment begins, someone should be checking social media and anonymous websites, like 4chan, Gab.ai and 8kun, which is how 8chan rebranded in 2019, for mentions of your name, address, phone number and portions of your address. 4chan and Gab.ai have policies against posting personal information, like emails, physical addresses, phone numbers or bank account information — a practice called doxing — and should remove identifying content when requested. Twitter, Facebook, LinkedIn and more popular social networks do, too. Also, set a Google alert for your name to see if you're being blogged about. If you or your newsroom can afford it, consider working with a security expert who knows how to monitor private Discord chat groups, private Facebook groups, 8kun, Telegram and other corners of the internet where harassment campaigns are hatched.

4 Know when to get law enforcement involved.

If a current or former address of yours begins to emerge online or if you're receiving threats of violence, call your local police non-

emergency line and let them know that an online troll may misreport an incident in the hopes of sending a team of armed police to your home — a practice known as swatting. Local police might not be accustomed to dealing with online threats or have a swatting protocol, but it's worth making a call and explaining the situation to ensure that unnecessary force is not deployed if a fraudulent report is made.

5 Save your receipts.

Check your email, check your bank account, and don't delete evidence of harassment. If you receive emails that your passwords for online accounts are being reset, do not click on or download anything. Save all emails related to the harassment, too, as you may wish to refer to them later to see if a pattern emerges. The evidence might also be important if you need to prove to a business or law enforcement that you were the subject of a targeted campaign. Continue to monitor your bank account to ensure that fraudulent charges aren't made and that your financial information is secure. Unfortunately, hacked credit cards and passwords abound online. You may decide to call your bank after being harassed and ask for a new debit card to be issued.

6 Let other journalists know what you're going through.

Remember, while it's important to stay physically safe, the emotional toll is real, too. There's no reason to go through online harassment alone. Don't hesitate to reach out to other journalists on your beat at different publications to let them know your situation. Stronger communities make for safer reporting.

Additional resources to support journalists covering hate online

Online Harassment Field Manual by PEN America
This extensive guide has fantastic recommendations for editors, managers, journalists, and family and friends of those targeted by online harassment. It also catalogues a range of tools and other resources for enhancing your online security.

Holistic Security Manual by Tactical Tech
A comprehensive resource with tips on digital security and mental health during when receiving threats online.

About the Author

April Glaser is an investigative journalist at NBC News, covering the technology industry and labor and workplace culture in Silicon Valley. Previously, she worked at *Slate*, *Recode*, and *Wired*, reporting on AI, disinformation and hate online, and social media platforms. Before journalism, Glaser worked at the Electronic Frontier Foundation and various other nonprofits focusing on technology policy. Glaser is a 2020 Joan Shorenstein fellow at the Shorenstein Center on Media, Politics and Public Policy, where *Journalist's Resource* is housed.

This tip sheet was developed in collaboration with Journalist's Resource at the Shorenstein Center with funding support from The MacArthur Foundation.